



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,292	06/06/2001	Gary Manuel Jackson	63795-0007	6320

24633 7590 06/17/2005
HOGAN & HARTSON LLP
IP GROUP, COLUMBIA SQUARE
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004

EXAMINER

JACKSON, JENISE E

ART UNIT PAPER NUMBER

2131

DATE MAILED: 06/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/874,292

Applicant(s)

JACKSON, GARY MANUEL

Examiner

Jenise E. Jackson

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____ | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-33 rejected under 35 U.S.C. 102(e) as being anticipated by Joyce(6,519,703).
3. As per claim 1, Joyce discloses a method for detecting unauthorized intrusion in a network system(see col. 1, lines 50-54, col. 3, lines 33-37, col. 4, lines 50-54), including the steps of: receiving packet level activity information from the network(see col. 1, lines 51-54, col. 2, lines 41-65); sorting port specific activity information from the received packet level activity information by IP/user(see col. 4, lines 13-16); converting the sorted IP/user port specific activity information to human behavioral measures of intent(see col. 2, lines 41-65, col. 3, lines 29-58). monitoring the converted human behavioral measures(see col. 2, lines 41-65, col. 3, lines 29-58, col. 4, lines 13-16, 50-54); and executing at least one of a blocking action based upon the monitored human behavioral measures(see col. 2, lines 51-54, col. 3, lines 1-16, 43-58).
4. As per claim 2, Joyce discloses wherein the step of monitoring includes: identifying presence of at least one activity from the port specific activity information(see col. 3, lines 29-58, col. 4, lines 13-16); assigning a binary representation (1=present, 0=absent) to the at least one identified activity; and generating an assessment based upon the binary rating, a binary rating is

Art Unit: 2131

inherent in a heuristic firewall, because packets are given ratings of whether they are harmful(see col. 1, lines 51-54, col. 2, lines 41-65).

5. As per claim 3, Joyce discloses wherein the step of generating an assessment includes associating the binary rating with an assessment based upon predetermined behavioral criteria (see col. 2, lines 41-65, col. 3, lines 29-58).

6. As per claim 4, Joyce discloses wherein the step of generating an assessment includes mapping the assessment on at least one two-dimensional grid(see col. 6, lines 30-46).

7. As per claim 5, Joyce discloses wherein the step of mapping occurs dynamically and in real-time(see col. 3, lines 29-58).

8. As per claim 6, Joyce discloses wherein the step of generating an assessment includes generating a profile of user based upon the monitored port specific activity information(see col. 4, lines 1-20).

9. As per claim 7, Joyce discloses wherein the step of generating an assessment is carried out utilizing a back propagation network(see col. 5, lines 61-67).

10. As per claim 8, Joyce discloses wherein the back propagation network includes psychological assessment information(see col. 2, lines 41-65, col. 5, lines 61-67).

11. As per claim 9, Joyce discloses wherein the assessment is one of high deception/high expertise, high deception/low expertise, low deception/high expertise and low deception/low expertise(see col. 2, lines 41-65, col. 3, lines 1-16).

12. As per claim 10, Joyce discloses wherein the blocking action includes sending a blocking command to a firewall for blocking further network access(see col. 3, lines 1-16, 43-58).

Art Unit: 2131

13. As per claim 11, Joyce discloses wherein the tracking action includes storing activity information in a tracking module(see col. 3, lines 1-28).

14. As per claim 12, Joyce discloses a traffic sorter that receives a copy of the network activity and sorts such activity by IP/users(see col. 3, lines 29-58); an activity monitor operatively coupled to the traffic sorter for monitoring converted human behavior measures by IP/users, that is based upon a copy of the network activity; an inter-port fusion module that fuses assessments from one or more assessment engines that monitor behavior measures by port and non-port specific behavior conversions; and an outcome director operatively coupled to the inter-port fusion monitor(see col. 3, lines 29-58, col. 4, lines 12-21).

15. As per claim 13, Joyce discloses wherein the activity monitor includes at least one dedicated port monitor(see col. 4, lines 13-16).

16. As per claim 14, Joyce discloses wherein, the at least one dedicated port monitor includes a packet level analysis module, an activity translator module and an assessment module(see col. 1, lines 50-55, col. 2, lines 41-65, col. 4, lines 13-16).

17. As per claim 15, Joyce discloses wherein the assessment nodule includes a back propagation network(see col. 5, lines 61-67).

18. As per claim 16, Joyce discloses wherein the back propagation network includes psychological assessment information(see col. 2, lines 41-65, col. 5, lines 61-67).

19. As per claim 17, Joyce discloses wherein the traffic sorter receives packet level activity information from the network and sorts the port specific activity information from the network see col. 3, lines 29-58, col. 4, lines 13-16).

Art Unit: 2131

20. As per claim 18, Joyce discloses wherein the activity monitor monitors the port specific activity information (see col. 4, lines 13-16).
21. As per 19, Joyce discloses wherein the activity translator module assigns a binary rating based upon presence (1) or absence (0) of at least one activity detected by the packet level analysis module(see col. 3, lines 29-58, col. 4, lines 13-16).
22. As per claim 20, Joyce discloses wherein the assessment module generates an assessment result based upon the binary rating(see col. 3, lines 29-58, col. 4, lines 13-16).
23. As per claim 21, Joyce discloses wherein the assessment module maps the assessment result utilizing at least one of a two dimensional grid or X dimensional grid for optional real-time viewing of a user's intent(see col. 3, lines 29-67).
24. As per claim 22, Joyce discloses wherein an outcome director initiates at least one of a blocking command or a tracking command based upon the assessment result(see col. 2, lines 41-65).
25. As per claim 23, Joyce discloses wherein the blocking command is directed to a system firewall(see col. 2, lines 30-65).
26. As per claim 24, Joyce discloses in which a blocking command results in the storage of all session data indicating all user activity and intent until such time as access is terminated(see col. 2, lines 41-65, col. 3, lines 29-67).
27. As per claim 25, Joyce discloses wherein the tracking command is directed to a tracking module (see col. 3, lines 1-28).
28. As per claim 26, Joyce discloses wherein the tracking module includes a tracking database for storing activity information that may be used to provide evidence of an intruder's

Art Unit: 2131

harmful intent activities and at least one intent assessment during a session (see col. 3, lines 1-28, col. 3, lines 29-58, col. 4, lines 13-16).

29. As per claim 27, Joyce discloses wherein the tracking database includes neural network assessment and associated information for the intruder that is at least one of tracked or blocked(see col. 2, lines 41-65).

30. As per claim 28, Joyce discloses wherein the tracking database includes a comparison module for comparing the neural network assessment and associated information against a second assessment based upon a second network intrusion(see col. 3, lines 29-67).

31. As per claim 29, Joyce discloses wherein at least one of a blocking or tracking action is executed based upon an output from the comparison module(see col. 3, lines 29-67, col. 4, lines 34-43).

32. As per claim 30, Joyce discloses sorting means for sorting port specific activity and across port specific activity from incoming packet level activity by IP/users; conversion means for converting the port specific activity and across port specific activity to behavioral measures of intent; monitoring means operatively coupled to the sorting means for monitoring the behavioral measures; and assessing means operatively coupled to the monitoring means for generating separate and independent IP/user assessments based upon the behavior measures (see col. 1, lines 50-55, col. 2, lines 41-65, col. 4, lines 13-16).

33. As per claim 31, Joyce discloses a computer usable medium having computer readable code embodied therein for preventing unauthorized intrusion into a computer network(see col. 1, lines 50-54, col. 3, lines 33-37, col. 4, lines 50-54), the computer program product comprising: computer readable program code configured to cause the computer to process a copy of network

Art Unit: 2131

activity in real-time to sort port specific and non-port specific activity information by IP/user from packet level activity information received by the computer network(see col. 1, lines 51-54, col. 2, lines 41-65); computer readable program code configured to cause the computer to covert the port and non-port specific activity information to behavioral measures of intent separately and independently for each IP/user(see col. 2, lines 41-65); computer readable program code configured to cause the computer to monitor behavior measures by IP/user(see col. 4, lines 13-16, 50-54); and computer readable program code configured to cause the computer to execute at least one of a blocking action or a tracking action for the IP/user if assessed behavioral measures indicate a threat intent(see col. 2, lines 51-54, col. 3, lines 1-16, 43-58).

34. As per claim 32, Joyce discloses wherein the step of receiving the port specific activity information includes creating a copy of the network activity sorted by users(see col. 3, lines 1-15).

35. As per claim 33, Joyce discloses the step of sorting non-port specific activity information from the received packet level activity information by the IP/user; and converting the non-port specific activity information to human behavioral measures of intent(see col. 2, lines 41-65, col. 3, lines 29-58).

Response to Amendment

36. The Applicant states that Joyce does not disclose detecting and monitoring various intrusion patterns or detecting new and previously undetected behaviors by separate IP/Users. The Examiner asserts that this is not claimed, and therefore, this remark is moot.

37. The Applicant states that Joyce fails to disclose a behavioral assessment method that is capable of converting the port specific activity information to behavioral assessment measures,

Art Unit: 2131

monitoring the behavior measures by IP/user and executing at least one of a blocking action or tracking action based upon the monitored behavior. The Examiner asserts that Joyce discloses behavioral assessment measures because Joyce discloses a heuristic firewall, that includes heuristic algorithms that include neural networks(see col. 2, lines 15-30). Thus, Joyce discloses an intrusion detection system that monitors packets for different types of intrusions, these intrusions that are submitted over the network in the form of packets, and these packets are submitted by hackers or crackers(see col. 2, lines 41-65, col. 3, lines 29-58). The behavior assessment is the packets that are submitted by hackers or crackers these packets are judged by the confidence level(see col. 2, lines 41-65). If the packets are deemed to be in low confidence, the packet are shunted out of the firewall(see col. 2, lines 51-54).

38. Joyce inherently discloses a traffic sorter because Joyce discloses that packets are deemed a confidence rating(see col. 3, lines 29-58). The data prep stages represent the inter-port fusion module that fuses assessments, because the data prep stages provide input data pre-processing, pulling out port from raw data packets to feed to a heuristic stage(see col. 4, lines 12-21).

Final Action

39. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period

Art Unit: 2131

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

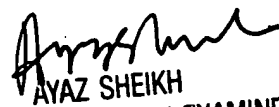
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



June 12, 2005



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100